CLAIMS

What is claimed is:

1. A method for booting a computer system, wherein the computer system includes a plurality of a devices, the method comprising the steps of:

(a) initiating a boot sequence in the computer system;

(b) determining whether a first device of the plurality of devices is one of a bootable device and a nonbootable device; and

(c) performing a clean restart of the boot sequence if the device is a nonbootable device, The method of claim 1, wherein the computer system further includes a BIOS and wherein the nonbootable device is bypassed during the clean restart.

2. An embedded security system coupled to the BIOS, wherein the embedded security system includes at least one protected control register dedicated to the boot sequence, and wherein the initiating step (a) further includes:

(a1) resetting a value in the at least one protected control register to zero;

(a2) hashing code in the BIOS to produce a BIOS digest value;

(a3) extending the BIOS digest value to the at least one protected control register; and

(a4) executing the code in the BIOS.

3. The method of claim 2, wherein the determining step (b) further includes:

(b1) hashing code in the first device to produce a device digest value;

(b2) extending the device digest value to the at least one protected control register;

(b3) executing the code in the first device; and

(b4) generating an interrupt signal if the first device is a nonbootable device.

4. The method of claim 3, wherein the computer system includes memory for storing the code loaded from the plurality of devices during the boot sequence, and wherein the step of performing a clean restart (c) further includes the steps of:

(c1) clearing the memory;

(c2) flagging the nonbootable device to instruct the BIOS to bypass the nonbootable device during the clean restart; and

(c3) repeating steps (a) and (b).

5. The method of claim 4 further including the steps of:

(d) booting the first device if the device is bootable, thereby booting an operating system.

6. The method of claim 5 further including the step of:

(e) verifying the trustworthiness of the boot sequence.

7. The method of claim 6, wherein the verifying step (e) further includes:

(e1) providing a predetermined value that represents a trustworthy boot sequence; and (e2) comparing the value of the at least one protected control register with the predetermined value.

8. The method of claim 2, wherein the BIOS includes a boot block and a main BIOS, and wherein the hashing step (a2) further includes:

(a2i) hashing code in the boot block to produce a boot block digest value;

(a2ii) extending the boot block digest value to the at least one protected control register;

(a2iii) executing the code in the boot block to transfer control to the main BIOS; and

(a2iv) hashing code in the main BIOS to produce a main BIOS digest value.

9. The method of claim 3, wherein the generating step (b4) further includes executing an INT 18h.

10. The method of claim 2, wherein the computer system includes a trusted computing platform in accordance with the standards defined by the Trusted Computing Platform Alliance (TCPA).

11. A system for booting a computer system, wherein the computer system includes a plurality of a devices, the system comprising:

a processor in the computer system;

a BIOS coupled to the processor for initiating and executing a boot sequence in the computer system;

wherein the BIOS determines whether a first device of the plurality of devices is one of a bootable device and a nonbootable device, and performs a clean restart of the boot sequence if the first device is a nonbootable device, bypassing the nonbootable device during the clean restart.

12. The system of claim 11 further including an embedded security system coupled to the BIOS, wherein the embedded security system includes at least one protected control register dedicated to the boot sequence, wherein a value in the at least one protected control register is reset to zero at initiation of the boot sequence, and wherein prior to executing code in the BIOS, the BIOS code is hashed to produce a BIOS digest value, which is extended to the at least one protected control register.

13. The system of claim 12, wherein the BIOS determines whether the first device is a nonbootable device by hashing code in the first device to produce a device digest value, extending the device digest value to the at least one protected control register, executing the code in the first device, and generating an interrupt signal if the first device is a nonbootable device.

14. The system of claim 13 further including memory coupled to the processor for storing code loaded from the plurality of devices during the boot sequence, and wherein if the interrupt signal is generated, the BIOS performs the clean restart by clearing the memory, resetting the value in the at least one protected control register to zero, and initiating a new boot

sequence, bypassing the nonbootable device.

15. The system of claim 14, wherein if the first device is bootable, the BIOS boots an operating system.

16. The system of claim 15, wherein the processor verifies the trustworthiness of the boot sequence.

17. The system of claim 16, wherein the processor is provided with a predetermined value that represents a trustworthy boot sequence, and the processor compares the value of the at least one protected control register with the predetermined value.

18. The system of claim 12, wherein the BIOS includes a boot block and a main BIOS and wherein code in the boot block is hashed and extended to the at least one protected control register before the boot block code is executed to transfer control to the main BIOS, and wherein code in the main BIOS is hashed and extended to the at least one protected control register before the main BIOS code is executed.

19. The system of claim 13, wherein the interrupt signal is an INT 18h.

20. The system of claim 12 further including a trusted computing platform in accordance with the standards defined by the Trusted Computing Platform Alliance (TCPA).

21. A computer readable medium containing programming instructions for booting a computer system, wherein the computer system includes a plurality of a devices, the programming instructions for:

(a) initiating a boot sequence in the computer system;

(b) determining whether a first device of the plurality of devices is one of a bootable device and a nonbootable device;

(c) performing a clean restart of the boot sequence if the first device is a nonbootable device, wherein the nonbootable device is bypassed during the clean restart.

22. The computer readable medium of claim 21, wherein the computer system further includes a BIOS and an embedded security system coupled to the BIOS, wherein the embedded security system includes at least one protected control register dedicated to the boot sequence, and wherein the initiating instruction (a) further includes instructions for:

(a1) resetting a value in the at least one protected control register to zero;

(a2) hashing code in the BIOS to produce a BIOS digest value;

(a3) extending the BIOS digest value to the at least one protected control register; and

(a4) executing the code in the BIOS.

23. The computer readable medium of claim 22, wherein the determining instruction (b) further includes instructions for:

(b1) hashing code in the first device to produce a device digest value;

(b2) extending the device digest value to the at least one protected control register;

(b3) executing the code in the device; and

(b4) generating an interrupt signal if the first device is a nonbootable device.

24. The computer readable medium of claim 23, wherein the computer system includes memory for storing the code loaded from the plurality of devices during the boot sequence, and wherein the instruction for performing a clean restart (c) further includes the instructions for:

(c1) clearing the memory;

(c2) flagging the nonbootable device to instruct the BIOS to bypass the nonbootable device during the clean restart; and

(c3) repeating instructions (a) and (b).

25. The computer readable medium of claim 24 further including the instructions for:

(d) booting the first device if the device is bootable, thereby booting an operating system.

26. The computer readable medium of claim 25 further including the instructions for:

(e) verifying the trustworthiness of the boot sequence.

27. The computer readable medium of claim 26, wherein the verifying instruction (e) further includes instructions for:

(e1) providing a predetermined value that represents a trustworthy boot sequence; and

(e2) comparing the value of the at least one protected control register with the predetermined value.

28. The computer readable medium of claim 22, wherein the BIOS includes a boot block and a main BIOS, and wherein the hashing instruction (a2) further includes instructions for:

(a2i) hashing code in the boot block to produce a boot block digest value;

(a2ii) extending the boot block digest value to the at least one protected control register;

(a2iii) executing the code in the boot block to transfer control to the main BIOS; and

(a2iv) hashing code in the main BIOS to produce a main BIOS digest value.

29. The computer readable medium of claim 23, wherein the generating instruction (b4) further includes the instruction for running an INT 18h.

30. The computer readable medium of claim 22, wherein the computer system includes a trusted computing platform in accordance with the standards defined by the Trusted Computing Platform Alliance (TCPA).